computer code that when executed on the processor causes the processor to if the data packet is encrypted, decrypt the data packet to produce a decrypted data packet.

68. The computer system as recited in claim 67, further comprising:
computer code that when executed on a computer causes the computer to decrypt the data packet using the encryption method.

69. The system as recited in claim 16, wherein the mechanism indirectly references said predetermined encryption/decryption mechanism.

70. The system as recited in claim 20, wherein the mechanism indirectly identifies the encryption method.

71. The method as recited in claim 26, wherein the mechanism indirectly identifies the encryption method.

72. The computer program product as recited in claim 36, wherein the mechanism indirectly identifies the encryption method.

73. The computer system as recited in claim 38, wherein the mechanism indirectly identifies the encryption method.

# REMARKS

In the Office Action, the Examiner rejected the claims under 35 USC § 251, 35 USC §112 and under 35 USC §102. These objections and rejections are fully traversed below.

The claims have been amended to correct minor informalities and to further clarify the subject matter regarded as the invention. Claims 1-73 are now pending.

Reconsideration of the application is respectfully requested based on the following remarks.

## OBJECTION RELATED TO REISSUE FORMALITIES

The Examiner notes that the original patent, or an affidavit or declaration as to loss or inaccessibility of the original patent, must be received before this reissue application can be allowed. Applicant previously submitted the original patent with Amendment A, submitted in response to the Office Action dated May 18, 1999. Accordingly, Applicant respectfully requests that the Examiner withdraw this objection.

## REJECTION OF CLAIMS 26-53 UNDER 35 USC §251

In the Office Action, the Examiner rejected claims 40-53 and 60-68 under 35 USC §251 as being an improper recapture of claimed subject matter cancelled in the application for the patent upon which the present reissue is based. As pointed out by the Examiner, original claims 6 and 14 were amended to specifically require that a new header be generated when the data packet is encrypted. As is understood by the Examiner, original claims 6 and 14 were directed at encryption of the data packet while the rejected claims 40-53 and 60-68 are directed to decryption rather than encryption. The Examiner has taken the position that amendments made to claims relating to encryption will and should have an estoppel effect on claims relating to decryption since encryption and decryption are essentially reverse processes of one another. Although one may be able to imagine situations where such an estoppel may be appropriate, it is respectfully submitted that such an estoppel is not appropriate in this case.

Specifically, claims 40-53 and 60-68 do recite a header. The feature that they do not recite is where the header is generated. It is acknowledged that in many (and probably most) situations, the header that is on the decrypted packet will have been generated by the encryption source. However, this is by no means a requirement. It is well known in the networking arts that there are a number of devices which strip a header and append a new header without affecting the data packet. For example, it is easy to contemplate a situation where a first node encrypts the data packet and appends an appropriate header to the encrypted data packet. The encrypted data packet is then forwarded to a second node which strips the header appended by the first node and appends its own header. From the standpoint of the device handling the decryption, it may be quite irrelevant which process or mechanism appended the header to the data packet that is being decrypted. Thus, in the present case, the

encryption and decryption are NOT necessarily mirror images of one another. Accordingly, it is respectfully submitted that in the present situation, amendments made to the encryption claims do not, and should not have an estoppel effect on the newly presented claims directed at decryption. Accordingly, it is respectfully submitted that claims 40-53 and 60-68 do not improperly recapture subject matter cancelled in the parent patent. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of claims 40-53 and 60-68 under 35 USC §251.

**REJECTION OF CLAIMS UNDER 35 USC §112**

In the Office Action, the Examiner rejected claims 1-15, 17-21, 30-33, 36-39, 44-46, and 50-53 under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Claim 20 has been amended in accordance with the Examiner's recommendations. In addition, claim 44 has been amended to further clarify the subject matter being claimed. However, claims 1 and 11 already conform to the Examiner's recommendations. Moreover, claim 54 does not include the language "said decryption key" as the Examiner indicated. In addition, claims 61 and 65 indicate that decryption is performed only when it is determined from the header section that the data packet is encrypted. This does not mean that a second decryption is performed. However, with reference to claim 18, decryption of the packet may also include decryption of the header of the data packet as well as the body of the data packet. Thus, the claim has not been amended to limit it to the more narrow interpretation that the Examiner has suggested. Moreover, with reference to claim 22, the claim recites "the address header including broadcast addresses of the first and second computers and the body including address information representing an internetwork address of the first computer and an internetwork address of the second computer, wherein the address information is encrypted." Thus, the address information is clearly defined in the claim and therefore the claim has not been amended. Hence, Applicant respectfully requests that the Examiner withdraw the rejection of the claims under 35 USC §112, second paragraph.

**REJECTION OF CLAIMS UNDER 35 USC §102**

In the Office Action, the Examiner rejected claims 32-33, 40-41, and 44-53 under 35 USC §102(b) as being anticipated by White (WO 92/02095). Applicant acknowledges that White discloses that the header identifies the node via which the packet enters and leaves the network. See White, col. 4, lines 11-15. However, the referenced claims require that the header section store a source identifier identifying a "broadcast address" of the source and/or a destination identifier identifying a "broadcast address" of the destination. The term "broadcast address" is known in the art to refer to an IP address used for transmitting packets to all hosts on a given network. In other words, through the use of a broadcast address, a single host cannot be identified. In practice, the host portion of a broadcast address typically contains all 1s or all 0s. White neither discloses nor suggests that the header identifies a *broadcast* address of at least one of the networks associated with the source and destination of the data packet. Rather, White requires that the header identify an actual node via which the packet enters and leaves the network, as described above. The present invention prevents using the address of a particular node, particularly a node responsible for encryption and decryption of the data packet. The presently claimed invention therefore provides greater protection against tapping into the network to decipher the nature of the information transmitted. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of claims 32-33, 40-41, and 44-53.

In addition, the Examiner rejected claims 1-73 under 35 USC §102(e) as being anticipated by Adams Jr. et al. ('782). This rejection is respectfully traversed. Adams Jr. discloses a computer network encryption/decryption device (CNEDD) that operates in one of two modes by selectively encrypting or decrypting packets based on information contained in a packet's header. See Adams Jr., Abstract. When the CNEDD operates in the standard mode, only the data portion of a packet is encrypted, and a new packet is transmitted which includes an unencrypted header (with the original routing information) and the encrypted data. See Adams Jr., col. 6, lines 63-68. In the tunneling mode, both the data characters and the header characters of a packet are encrypted. See Adams Jr., col. 6, line 68 – col. 7, line 2. In addition, encryption and decryption is performed based on information contained in a table, as described in Adams. See Adams Jr., col. 7, lines 17-41. Rather than including the routing information from the original data packet in the header of the encrypted packet, the header indicates that the source of the packet is a CNEDD and the destination of the packet is

a CNEDD in the network which contains the intended target node. See Adams Jr., col. 9, line 57-col. 10, line 2.

Claims 1, 6, 11, 16, and 17, as amended, are drawn to a method or system adapted for encrypting a data packet according to a predetermined encryption/decryption mechanism, generating a new header including a mechanism for identifying the predetermined encryption/decryption mechanism and appending the new header to the encrypted data packet.

Similarly, claims 20 and 24 are drawn to a method or system for decrypting a data packet including a header that includes a mechanism for identifying an encryption method used to encrypt the data packet.

Claims 26, 36, and 38, as amended, are drawn to a method, computer program product, or computer system adapted for encrypting data packets. When a data packet is encrypted, a new header is generated and appended to the encrypted data packet. The new header includes a mechanism for identifying an encryption method used to generate the encrypted data packet. For instance, the mechanism may (but does not need to) be a Security Parameters Index which specifies which "row" of a Security-Association Table a receiver should use to interpret the received packet. Thus, through the identification of an entry in a Security-Association Table, an encryption method used to generate the encrypted data packet may be identified. As a result, the presently claimed invention permits the encryption method to be tailored for each packet transmitted rather than requiring that the encryption method be specified statically (e.g., according to the source and/or destination of the packet).

The Examiner refers to Adams Jr. and states that indicating in the header whether the data packet is encrypted and the number of padding bytes used in the encryption identifies an encryption method. Applicant respectfully traverses this assertion. Col. 8, lines 5-14 state: "If DES encryption is used, the amount of information to be encrypted per packet must be in multiples of 8 bytes. That is, the length of data characters 70 must be either 8, 16, 32, etc. bytes long for the DES encryption to be performed properly. If the amount of information to be encrypted is not a multiple of 8 bytes, "padding" bytes are added to increase the length of the information block before encryption takes place. This use of padding bytes is well known to those skilled in the art." Adams Jr. neither discloses nor suggests that the indication of the number of padding bytes is used to identify an encryption method. As described above, the number of bytes in a packet may vary when DES encryption is used. Thus, Adams Jr. merely

implies that DES decryption may be performed properly through the identification of the number of padding bytes in the header of the encrypted data packet. Only one encryption method, DES, is discussed. Moreover, it is important to note that a variety of encryption methods may also require that the amount of information encrypted per packet be in multiples of 8 bytes long for the encryption to be performed properly, as described above with respect to DES encryption. Since there need not be a one-to-one correspondence between the encryption method and the number of padding bytes, the mere indication of the number of padding bytes cannot identify, either directly or indirectly, the encryption method used.

None of the cited references, separately or in combination, disclose or suggest a mechanism for identifying an encryption/decryption method in a header of the encrypted data packet. Similarly, none of the cited references disclose or suggest decrypting a data packet that has a header including a mechanism for identifying the encryption method used to encrypt the data packet. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of independent and dependent claims 1-6, 9-13, 16-17, 20, 24-31, 34-39, 54-55, and 60-73.

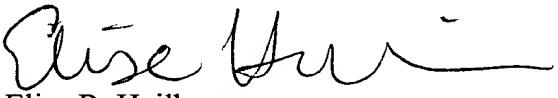
Claims 7-8, 14-15, 18-19, 21-23, 32-33, 40-53, and 56-59 are all drawn to a method, system or computer program product in which the broadcast address of at least one of the networks associated with the source and destination of the data packet are identified in a header of the data packet. Adams Jr. states that it is preferred that the new header indicates that the source of the packet is CNEDD and the destination of the packet is a CNEDD in the network which contains the intended target node. See Adams Jr., col. 9, line 66-col. 10, line 2. However, Adams Jr. neither discloses nor suggests that the new header include broadcast addresses of the source and the destination rather than the addresses of the devices that are responsible for encryption and decryption of the data packet. The presently claimed invention therefore provides greater protection against tapping into the network to decipher the nature of the information transmitted. Accordingly, Applicant respectfully submits that claims 7-8, 14-15, 18-19, 21-23, 32-33, 40-53, and 56-59 are patentable over Adams Jr.

**SUMMARY**

Reconsideration of the application and an early Notice of Allowance are earnestly solicited. If there are any issues remaining which the Examiner believes could be resolved through either a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned attorney at the telephone number listed below.

Applicants hereby petition for an extension of time which may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 50-0388 (Order No. SUN1P342R).

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP



Elise R. Heilbrunn
Reg. No. 42,649

BEYER WEAVER & THOMAS, LLP
P.O. Box 130
Mountain View, CA 94042-0130
Tel. (510) 843-6200